BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 14-111

18 MAY 2012

Incorporating Change 1, 16 June 2014

AIR FORCE MATERIEL COMMAND Supplement

25 FEBRUARY 2015

Intelligence

INTELLIGENCE SUPPORT TO THE ACQUISITION LIFE-CYCLE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-Publishing.af.mil** for downloading and ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/A2DP

Certified by: AF/A2D (Brig Gen Mark W. Westergren)

Supersedes: AFI 14-111, 10 January 2005

Pages: 34

(AFMC)

OPR: HQ AFMC/A2X

Certified by: HQ AFMC/A2X (Jonathan R. May)

Supersedes: AFI14-111_AFMCSUP, 23 March 2006

Pages:11

This publication implements Air Force Policy Directive (AFPD) 14-1, *Intelligence, Surveillance, and Reconnaissance (ISR) Planning, Resources, and Operations*, and is consistent with Department of Defense Instruction (DoDI) 5200.39, *Critical Program Information (CPI) Protection Within the Department of Defense*, AFPD 10-9 *Lead Command Designation and Responsibilities for Weapons Systems*, AFPD 16-7, *Special Access Programs*, AFPD 63-1, *Acquisition and Sustainment Life Cycle Management*, AFPD 99-1, *Test and Evaluation Process*, and AFPD 90-11, *Strategic Planning System*, and guidance portion in Department of Defense Directive (DoDD) 5250.01, *Management of Intelligence Mission Data (IMD) Within the DoD*. This publication must be used in conjunction with Air Force Instruction (AFI) 10-601, *Operational Capability Requirements Development*, AFI 14-132, *Air Force Geospatial Intelligence (GEOINT)*, AFI 14-201, *Intelligence Production and Applications*, AFI 14-205, *Geospatial Information and Services*, *Operational Capability Requirements Development*, AFI

63-101, *Acquisition and Sustainment Life Cycle Management,* AFI 63-114, *Quick Reaction Capability Process,* AFI 99-103, *Capabilities-Based Test and Evaluation,* AFI 99-114, *Foreign Materiel Program*. This publication applies to Regular Component, Air Force Reserve (AFR), Air National Guard (ANG), and Department of the Air Force (AF) Civilians. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Disposition Schedule (RDS) located in the Air Force Records Information Management System (AFRIMS). Submit change recommendations using an AF Form 847, *Recommendation for Change of Publication* to the Office of Primary Responsibility (OPR). This publication may be supplemented, but all supplements must be coordinated with the Office of Primary Responsibility (OPR) prior to certification and approval. Upon publication, MAJCOMS will ensure copies are provided to the OPR. Compliance waiver requests must be submitted through the chain of command to the appropriate tier waiver approval authority, all other waivers will be submitted to the publication OPR.

(AFMC) This publication implements Air Force Policy Directive (AFPD) 14-1, *Intelligence, Surveillance, and Reconnaissance (ISR) Planning, Resources, and Operations*, and further articulates AFI 14-111, *Intelligence Support to the Acquisition Lifecycle* for AFMC. It is consistent with Department of Defense Instruction (DoDI) 5200.39, *Critical Program Information (CPI) Protection Within the Department of Defense,* AFPD 10-9 *Lead Command Designation and Responsibilities for Weapons Systems*, AFPD 16-7, *Special Access Programs*, AFPD 63-1, *Integrated Life Cycle Management*, AFPD 99-1, *Test and Evaluation*, and AFPD 90-11, *Strategic Planning System,* and guidance portion in Department of Defense Directive (DoDD) 5250.01, *Management of Intelligence Mission Data (IMD) In DoD Acquisition*. This publication must be used in conjunction with Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3312.01B, *Joint Military Intelligence Requirements Certification,* Air Force Instruction (AFI) 10-601, *Operational Capability Requirements Development*, AFI 14-132, *Geospatial Intelligence (GEOINT),* AFI 14-205, *Geospatial Information and Services (GI&S)s,* AFI 61-101, *Management of Science and Technology*, AFI 63-101/20-101, *Integrated Life Cycle Management,* AFI 63-1201, *Life Cycle Systems Engineering*; AFI 63-131, *Modification Management*, AFI 99-103, *Capabilities-Based Test and Evaluation*, AFI 99-114, *Foreign Materiel Program*.

(AFMC) This publication applies to all AFMC Air Force (AF) active duty members and civilian employees, the Air Force Reserve, and the Air National Guard. Applicable organizations include AFMC Headquarters, Air Force Life Cycle Management Center (AFLCMC), Air Force Nuclear Weapons Center (AFNWC), Air Force Research Laboratory (AFRL), Air Force Sustainment Center (AFSC) and Air Force Test Center (AFTC). Specific processes and/or paragraphs supplemented in this publication may not be applicable to all Center/unit intelligence functions. Lower level supplement to this publication is not permitted. Refer recommended changes and updates to this publication to HQ AFMC/A2X using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847s from the field through the appropriate functional chain of command. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. (Ensure you properly Tier your product in accordance with AFI33-360.) See AFI 33-360, *Publications and Forms Management*, for a description of the authorities associated with the Tier numbers. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).

SUMMARY OF CHANGES

This interim change identifies tiered waiver authorities for unit level compliance items to depict the assessed risk of non-compliance and updates the certifying official. A margin bar (|) indicates newly revised material.

(AFMC) AFI 14-111 was substantially revised as of 18 May 2012. This supplement was revised accordingly and incorporates numerous changes throughout. This document must be completely reviewed to gain a full perspective of the changes. Major changes include: roles and responsibilities, key acquisition intelligence process and concept revisions, terminology updates and a title change. The word “program” is used in the instruction to refer to those activities requiring intelligence support.

1. ACQUISITION INTELLIGENCE

1.1. **Purpose.** Successful development of weapons systems, new operational concepts, and innovative combat techniques depends upon rapid, precise, accurate, and detailed intelligence, along with the infrastructure needed to provide it. Three key processes in the Department of Defense (DoD) must work in concert to deliver the capabilities required by the warfighter: The requirements process, the acquisition process and the Planning, Programming, Budget and Execution (PPBE) process. Acquisition intelligence activities span all three processes, as well as additional processes that are unique to the Intelligence Community (IC). Intelligence Supportability Analysis (ISA) is the process by which AF intelligence, acquisition and operations analysts identify, document and plan for requirements, needs and supporting intelligence infrastructure necessary to successfully acquire and employ AF capabilities, thereby ensuring intelligence supportability. ISA is required throughout a program’s life cycle, and should be considered for all programs and initiatives. This publication outlines processes and provides guidance to ensure intelligence and its related infrastructure are aligned and integrated appropriately within AF acquisition-related activities.

1.1.1. **(Added-AFMC)** Special Access Programs (SAPs). This AFMC supplement provides AFMC-specific guidance on acquisition intelligence operations and responsibilities. All SAPs are to comply with this AFMC supplement. AFMC/A2/5, AFLCMC, AFNWC, AFRL, AFSC or AFTC SAP cleared personnel will evaluate intelligence needs of SAPs and recommend SAP program managers include appropriate acquisition intelligence analysts to ensure intelligence requirements are addressed.

1.1.2. **(Added-AFMC)** Acquisition Intelligence Guidebook (AIG). The AIG provides detailed instructions and tools which can be tailored to integrate intelligence data and services into the design, analysis, planning, testing, risk mitigation and resource decisions executed by program offices.

1.2. **Objective.** To support effective research, development, fielding, employment, sustainment and improvement of AF capabilities by identifying intelligence requirements, resolving/mitigating deficiencies, integrating intelligence, and providing needed intelligence data and infrastructure in a timely and secure manner.

1.3. **Tenets.** Effective acquisition intelligence support is:

1.3.1. Relevant, providing meaningful support that enables programs to optimize capabilities.

1.3.2. Iterative, providing timely intelligence inputs to the materiel effort along acquisition timelines in an evolving fashion dictated by materiel development and sustainment needs.

1.3.3. Tailored, focusing products and processes to meet the needs of the users while reducing extraneous information.

1.3.4. Collaborative. Requiring partnership across acquisition, intelligence, counterintelligence, and requirements communities in order to identify and resolve intelligence issues related to new and evolving programs.

2. ROLES AND RESPONSIBILITIES

2.1. General

2.1.1. USAF Intelligence Offices are the primary interface to the National Intelligence Community and will partner with the IC to provide intelligence products and services, and to identify and resolve the intelligence needs of AF programs.

2.1.2. Authoritative threat intelligence information will be used by AF programs when validated intelligence information is not required. The National Air and Space Intelligence Center (NASIC) and other DoD/Service intelligence production centers provide authoritative threat intelligence information suitable for program use.

2.2. **Administrative Assistant to the Secretary of the Air Force (SAF/AA)** Serves as the Senior Security Official for the AF with oversight and policy authority for all AF SAPs.

2.3. **Assistant Secretary of the Air Force for Acquisition (SAF/AQ):** Sets policy and direction for AF acquisition processes to ensure intelligence dependencies, shortfalls and requisite courses of action are identified to resolve shortfalls for intelligence-sensitive programs.

2.4. **Deputy Chief of Staff, Intelligence, Surveillance, and Reconnaissance (AF/A2):**

2.4.1. Sets policy and direction for AF intelligence processes to ensure intelligence products and services are integrated across the full acquisition life cycle. This includes research, development, acquisition, test, modernization and sustainment activities.

2.4.2. Provides oversight of the processes and procedures governing derived intelligence requirements.

2.4.3. Participates in the development of, and reviews requirements, planning, and acquisition documents and ensures they adequately address intelligence interests and have appropriate intelligence content.

2.4.4. Collaborates with AF/A3/5 and SAF/AQ to provide intelligence support during development of new requirements and program documents.

2.4.5. Represents AF ISR interests with respect to DoD and other agency activities impacting AF acquisition intelligence programs.

2.4.6. Collaborates with Intelligence Agencies and across AF staffs to establish policies for threat Modeling & Simulation (M&S) efforts.

2.4.7. Establishes workforce standards for acquisition intelligence competencies to include initial certification and recurring training, as appropriate. Approval authority for Major Command (MAJCOM) requests for waivers to acquisition intelligence certification requirements.

2.4.8. Advises the Director of Acquisition Career Management on acquisition intelligence workforce management issues, and assists in execution of acquisition workforce responsibilities in respective acquisition functions IAW AFI 36-2640, *Executing Total Force Development*.

2.4.9. Ensures collaboration between the IC and AF requirements, planning and acquisition communities in the development and sustainment of warfighting capabilities.

2.4.10. Provides intelligence certification recommendation as part of Joint Capabilities Integration and Development System (JCIDS) coordination and leverages acquisition intelligence inputs such as Independent Intelligence Assessment (IIA) to develop certification recommendations.

2.4.11. IAW AFPD 16-7, advocates intelligence requirements, provides substantive intelligence support, oversees acquisition intelligence support and provides intelligence oversight for all SAPs.

2.5. **Deputy Chief of Staff, Operations, Plans and Requirements (AF/A3/5):**

2.5.1. Ensures intelligence dependencies are described within applicable JCIDS documents per Joint Staff guidance and addressed within the AF Requirements Oversight 144 Council requirements approval process.

2.5.2. Collaborates with AF/A2 for intelligence support on issues concerning system performance, system survivability and validation of operational survivability requirements as well as on Planning and direction, Collection, Processing and exploitation, Analysis and production, and Dissemination (PCPAD) architectures and supportability.

2.5.3. Ensures that AF/A2 participates in the development and review of requirements, planning, and acquisition documents to ensure they adequately address intelligence interests, concept of operations (CONOPS), and have appropriate intelligence content.

2.5.4. Coordinates JCIDS documents with AF/A2 for intelligence certification recommendation prior to forwarding for Joint Staff intelligence certification.

2.5.5. As lead for AF M&S policy and standards, collaborates with AF/A2 and NASIC to establish policy for threat M&S efforts, to include those performed in support of program-based requirements development and simulation-based support activities throughout the life cycle.

2.6. **MAJCOM/Field Operating Agency (FOA):**

2.6.1. Identify ISR subject matter experts (SMEs) (to include acquisition intelligence specialists) and process owners to support requirements development High-Performance Team (HPT) processes. (T-2)

2.6.1.1. **(Added-AFMC)** Center Senior Intelligence Officers (SIOs) will ensure qualified SMEs are available to support AFMC requirements development HPTs. **(T-2).**

2.6.1.2. **(Added-AFMC)** Center SIOs will ensure that SMEs are prepared for HPT participation. Center SIOs will ensure SMEs obtain appropriate HPT training as per the AFMC Supplement to AFI 10-601 (paragraph 2.5.3.) to ensure readiness to participate in HPTs. **(T-2).**

2.6.1.3. **(Added-AFMC)** Center SIOs will maintain a roster of ISR SMEs, to include inputs of qualified Air Force Reserve personnel aligned to support the Center's mission, identifying their areas of expertise and HPT training status should be done in collaboration respectively with supporting Reserve unit and IMA leadership. Center SIOs will provide the SME roster to HQ AFMC/A2/5, and courtesy copy the AFRC/A2. **(T-2).**

2.6.2. Ensure timely, complete, sufficient, and accurate intelligence analysis, information and support is provided to and integrated within capabilities-based planning and requirements development processes and life cycle PPBE documentation. (T-2)

2.6.2. **(AFMC)** AFMC Center SIOs will support AFMC and PM requirements to ensure timely, complete, sufficient, and accurate intelligence analysis, information and support is provided to and integrated within AFMC's capabilities-based planning and requirements development processes and life cycle PPBE documentation. **(T-2).**

2.6.3. Provide initial certification of personnel as acquisition intelligence specialists based upon the following minimum requirements: (1) completion of Defense Acquisition University courses ACQ 101, *Fundamentals of Systems Acquisition Management* and RQM 110, *Core Concepts for Requirements Management,* (2) completion of the Acquisition Intelligence Formal Training Unit, (3) one year experience in a designated acquisition intelligence position. Submit requests for waivers to initial certification requirements to MAJCOM/FOA A2. (T-2)

2.6.3. **(AFMC)** Fundamentals of Systems Acquisition Management (ACQ 101) and Intelligence in Acquisition Life-Cycle Management (SYS 031) are pre-requisites for enrollment in the Acquisition Intelligence Formal Training Unit. Introduction to the Joint Capabilities Integration & Development System (CLR 101) is a pre-requisite for Core Concepts for Requirements Management (RQM 110). **(T-2).**

2.6.4. Collaborate with AF/A2 to designate positions as acquisition intelligence positions. (T-2)

2.6.5. Participate in acquisition intelligence activities as follows:

2.6.5.1. Assist in the MAJCOM/FOA development of strategic plans and other acquisition-related documents, studies and analyses, ensuring ISR requirements and constraints are addressed. (T-2)

2.6.5.2. Participate in identification of intelligence support requirements for intelligence-sensitive acquisition programs. (T-2)

2.6.5.2. **(AFMC)** AFMC Center SIOs will be the OPR at each Center for identification of intelligence support requirements for intelligence-sensitive acquisition programs. **(T-2).**

2.6.5.3. Draft and coordinate intelligence content for JCIDS and other requirements, acquisition and program planning documents for completeness, supportability, impact, and threat content. (T-2)

2.6.5.3. **(AFMC)** AFMC Center SIOs will coordinate with AFMC A2/5 and PMs regarding intelligence content for JCIDS and other requirements, acquisition and program planning documents for completeness, supportability, impact, and threat content. **(T-2).**

2.6.5.4. Coordinate analysis of requirements to identify ISR-related deficiencies and guide efforts to resolve those deficiencies. (T-2)

2.6.5.4. **(AFMC)** AFMC Center SIOs will support AFMC and PM requirements to identify, document and resolve ISR-related deficiencies. **(T-2).**

2.6.5.5. Participate in acquisition intelligence forums, as appropriate (e.g., Intelligence Support Working Group (ISWG), Threat Steering Group (TSG), etc.) to support derivation of intelligence requirements, intelligence costing, assessment of data shortfalls, and development of courses of action to address shortfalls. (T-2)

2.6.5.6. Coordinate with implementing command A2 to determine acquisition intelligence lifecycle support required for intelligence-sensitive materiel requirements (rapid reaction, modernization and sustainment, acquisition etc.). (T-2)

2.6.5.7. Submit requirements for and/or assist in the justification of requirements for modifications to fielded programs, based on emerging threats or technologies that jeopardize the mission effectiveness or survivability of the system. (T-2)

2.7. **Program Executive Officers (PEOs), Technology Executive Officer, Designated Acquisition Officials (DAOs) and PMs.**

2.7.1. In collaboration with implementing command designated intelligence focal points, ensure programs within their responsibility receive appropriate acquisition intelligence support IAW AFI 14-111 and AFI 63-101.

2.7.2. Determine Program Protection Plan (PPP) intelligence requirements IAW DoDI 5200.39. (T-0)

2.7.3. **(Added-AFMC)** Center SIOs are the designated intelligence focal point for these actions. **(T-2).**

2.8. **Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISRA). In addition to FOA responsibilities, AFISRA also:**

2.8.1. Through NASIC, provide air, space and cyber intelligence assessments, products and services for a wide range of needs. (T-3)

2.8.1.1. Ensure NASIC chairs and/or attend TSGs. (T-3)

2.8.1.2. NASIC, as lead AF agency for production of Capstone Threat Assessments (CTAs), System Threat Assessments (STAs) and System Threat Assessment Reports (STARs), validate all intelligence production requirements (PR) and broker/monitor status of such requirements for satisfaction through the Defense Intelligence Analysis Program (DIAP). NASIC is the AF validation authority for Acquisition Category (ACAT) IC and ACAT II authoritative threat documents. NASIC is also responsible for applying the analysis of other national, DoD agencies/organizations, or allied intelligence services, as needed, to meet the need of the USAF force modernization and acquisition communities. (T-3)

2.8.1.3. Identify data production capabilities and shortfalls impacting acquisition programs. Identify associated operational impacts to support risk assessments and course of action development. (T-2)

2.8.1.4. Collaborate with AF/A2 and AF/A3/5, to establish standards for threat M&S efforts, to include those performed in support of program/capability-based requirements development and simulation-based support activities throughout the life cycle. (T-3)

2.8.1.5. Review threat and life-cycle intelligence mission data plans/documents/studies/ assessments prior to milestone (MS) reviews, as required. Ensure threat and intelligence mission data information meet DoD and AF standards. (T-2)

2.8.1.6. Monitor Critical Intelligence Parameters and provide appropriate notification in case of a breach. (T-2)

2.9. **Implementing Command (Air Force Material Command (AFMC), Air Force Space Command (AFSPC)):**

2.9.1. Ensure ready forces and capabilities (to include tools) to execute their acquisition intelligence mission. (T-2)

2.9.1.1. Collaborate with AF/A2 to establish workforce training standards for acquisition intelligence competencies, to include initial certification and recurring training, as appropriate. (T-2)

2.9.1.1.1. **(Added-AFMC)** AFMC/A2/5 will determine acquisition intelligence training and certification requirements for all AFMC intelligence personnel and will promulgate said requirements in the AFMC Training Standard. AFMC/A2/5 will provide updated certification instructions and requirements to the Center SIOs as needed. **(T-2).**

2.9.1.2. Lead development of curricula for Acquisition Intelligence Formal Training Unit. (T-2)

2.9.1.2. **(AFMC)** The AFLCMC Intelligence Directorate's 21st Intelligence Squadron (formerly the AFMC Intelligence Squadron) is the OPR for the Acquisition Intelligence Formal Training Unit. **(T-2).**

2.9.1.3. Provide initial certification of personnel as acquisition intelligence specialists based upon the following minimum requirements: (1) completion of Defense Acquisition University courses ACQ 101, Fundaments of Systems Acquisition Management and RQM 110, Core Concepts for Requirements Management (2) completion of the Acquisition Intelligence Formal Training Unit (3) one year experience in a designated acquisition intelligence position. (T-2)

2.9.1.3.1. **(Added-AFMC)** In addition to the requirements identified in AFI 14-111 paragraph 2.9.1.3., AFMC/A2, with the support from AFMC Center SIOs, will identify, develop and deliver training and certification requirements for Initial Qualification Training (IQT) and Mission Qualification Training (MQT) per AFI 14-202, for AFMC acquisition intelligence designated personnel. **(T-2).**

2.9.1.4. Maintains and updates, the Acquisition Intelligence Guidebook (AIG), as required. The guidebook serves as a reference on intelligence tasks throughout the life cycle of an acquisition program or project and is available from AFMC/A2X. (T-3)

2.9.1.4.1. **(Added-AFMC)** AFLCMC/IN will develop, produce, maintain and update an Acquisition Intelligence Guidebook (AIG) in coordination with AFMC intelligence units. AFI 14-111, AFMC Supp 14-111 and the AFMC Acquisition Intelligence Guidebook (AIG) are a triad of complementary documents designed to work in concert. It is recommended that AFMC personnel refer to all three of these publications for a complete picture of acquisition intelligence definitions, concepts, policies, processes, procedures and requirements. **(T-3).**

2.9.1.5. **(Added-AFMC)** AFMC/A2/5 will facilitate communication of acquisition intelligence topics to Air Education And Training Command (AETC) for incorporation into intelligence basic and follow-on course curricula. **(T-2).**

2.9.2. Ensure timely, complete, sufficient, and accurate intelligence analysis, information and support are provided to and integrated into acquisition and sustainment processes. (T-2)

2.9.2. **(AFMC)** AFMC Center SIOs will support MAJCOM/FOA sponsor and PM requirements to ensure timely, complete, sufficient, and accurate intelligence analysis, information and support are provided to and integrated into research, development, acquisition, test, sustainment and SAP activities and processes. AFMC Center SIOs will partner with Center PMs and establish program/activities prioritization based on intelligence sensitivity and work with Center PMs to identify resource strategy. **(T-2).**

2.9.2.1. **(Added-AFMC)** Intel support is primarily provided through the Intelligence Supportability Analysis (ISA) process. AFMC Center SIOs shall conduct ISA for all

Tier I intelligence sensitive programs as defined in the AIG. Every effort shall be given to provide ISA to lower tier programs based on local prioritization and resource strategy. The AIG contains detailed descriptions, processes, procedures and tools for conducting ISA. ISA can be applied to all AFMC efforts, including but not necessarily limited to: **(T-2).**

2.9.2.1.1. **(Added-AFMC)** Acquisition Programs (ACAT or Non-ACAT)

2.9.2.1.2. **(Added-AFMC)** Sustainment efforts/programs

2.9.2.1.3. **(Added-AFMC)** Quick Reaction Capabilities (QRCs)

2.9.2.1.4. **(Added-AFMC)** Joint Urgent Operational Needs (JUONs)

2.9.2.1.5. **(Added-AFMC)** Development Planning (DP) efforts

2.9.2.1.6. **(Added-AFMC)** Technology Development

2.9.2.1.7. **(Added-AFMC)** AFRL initiatives

2.9.2.1.8. **(Added-AFMC)** Foreign Military Sales (FMS) programs

2.9.2.1.9. **(Added-AFMC)** Test efforts/programs

2.9.2.1.10. **(Added-AFMC)** Analysis of Alternatives (AoAs)

2.9.2.2. **(Added-AFMC)** AFMC Center SIOs will provide acquisition intelligence support in accordance with AFI 63-101/20-101, AFI 63-131, and AFI 63-114. **(T-2).**

2.9.2.3. **(Added-AFMC)** Recommended guidance on performing acquisition intelligence support is located in the Acquisition Intelligence Guidebook (AIG).

2.9.3. In collaboration with the lead command A2 and programs, performs objective assessments of intelligence impacts associated with intelligence-sensitive programs from both an impact to acquisition and impact to operational employment perspective. (T-2)

2.9.3. **(AFMC)** AFMC Center SIOs will partner with PMs to ensure risk associated with intelligence-sensitive programs is considered as part of a program’s overall risk assessment. AFMC Center SIOs will perform Intelligence Health Assessments as part of their acquisition intelligence support activities. **(T-2).**

2.9.3.1. Documents identify impact in IIA and provide that information to AF/A2 to support intelligence certification recommendations as well as other Headquarters AF and DoD level planning and requirements activities. (T-2)

2.9.4. Oversee and manage the conduct of acquisition intelligence, as follows:

2.9.4.1. Determine intelligence sensitivity of programs and advise program offices and MAJCOMs/FOAs (for new programs) of corresponding levels of support required to execute acquisition intelligence responsibilities. This information supports development of acquisition program baselines that account for program office intelligence workload. (T-1)

2.9.4.1.1. **(Added-AFMC)** AFMC Center SIOs will review the intelligence needs of all programs across the entire acquisition and sustainment lifecycle to determine intelligence sensitivity. This high-level assessment will be used to establish program/activity prioritization for more thorough support efforts. **(T-1).**

2.9.4.1.2. **(Added-AFMC)** AFMC Center SIOs will maintain information and metrics on program intelligence sensitivity. Semi-annually, AFMC Center SIOs will provide AFMC/A2/5 with program intelligence sensitivity information and metrics. **(T-1).**

2.9.4.2. Oversee and review completion of ISA for programs to include documentation of intelligence requirements, deficiencies, and proposed solutions. This must be accomplished for programs in all phases including technology development, acquisition, test and sustainment. (T-2)

2.9.4.3. Work with PEOs/DAOs to identify requirements for acquisition intelligence related program facilities, personnel and resources. (T-2)

2.9.4.3. **(AFMC)** AFMC/A2 will work with AFMC Center SIOs and the Program Managers to identify required facilities, personnel and resources needed to provide adequate acquisition intelligence and special security office support throughout the program's life cycle. This should happen as early as possible in the acquisition lifecycle in preparation for program transitions (e.g. one center to another or as programs transition the lifecycle) to facilitate PPBE actions to attain resources. **(T-2).**

2.9.4.4. Identify and submit intelligence PRs to initiate IC production processes. (T-1)

2.9.4.4.1. **(Added-AFMC)** AFMC Center SIOs will identify and submit threat and intelligence mission data production requirements through COLISEUM and/or through processes established in DoDD 5250.01; CJCSIs 3170 and 3312.01; and AFIs 10-601 and 63-101/20-101. **(T-1)**.

2.9.4.4.2. **(Added-AFMC)** AFMC Center SIOs will identify and submit Geospatial Intelligence (GEOINT) requirements through processes established in AFIs 14-132 and 14-205. **(T-1).**

2.9.4.5. Obtain expertise and cost data from intelligence agencies, as necessary. Work with acquisition counterparts (program manager (PM), Technology Lead, etc.) and MAJCOMs/FOAs to ensure intelligence costs are included in life cycle cost estimates and program budgets. (T-3)

2.9.4.5. **(AFMC)** AFLCMC/IN is the Command focal point for acquisition intelligence costing and will directly provide costing assistance to Center SIOs as required. **(T-3).**

2.9.4.6. Provide intelligence input to command attestation/certification of acquisition requirements feasibility. (T-2)

2.9.4.6. **(AFMC)** AFMC requirements attestation/certification process description and responsibilities can be found in AFMC Supp 10-601, paragraph 3.3.17.10. **(T-2).**

2.9.4.7. Provide intelligence analytical support to capabilities-based planning activities, as required. (T-2)

2.9.4.7. **(AFMC)** Center SIOs will provide support to capabilities-based planning and development planning activities. Recommended guidance is located in the AFMC Developmental Planning Guide. Center SIOs will also provide support to capabilities-based planning through participation in the ISA process. ISA results will contribute to the needs and solution processes. **(T-2).**

2.9.4.8. Perform Cross-Program Analysis (CPA) of program derived intelligence requirements to ensure consolidation of common deficiencies and facilitate development of multi-program solutions. Provide resulting derived requirements to appropriate MAJCOMs/FOAs for resolution via established AF requirements processes as well as to IC agencies for resolution via established intelligence PRs processes. (T-3)

2.9.4.8.1. **(Added-AFMC)** AFMC Center SIOs will perform CPA on programs within their respective portfolios. **(T-3).**

2.9.4.8.2. **(Added-AFMC)** AFMC Center SIOs will provide results of portfolio CPAs to AFLCMC/IN. In turn, AFLCMC/IN will provide feedback on the results of any cross-center CPAs. **(T-3).**

2.9.4.8.3. **(Added-AFMC)** AFMC Center SIOs are responsible for executing and documenting CPA within their respective portfolios. AFMC/A2/5 has delegated AFMC-wide CPA to AFLCMC/IN. AFLCMC/IN will maintain CPA documentation. **(T-3).**

2.9.4.9. Ensure acquisition intelligence specialists participate in force modernization forums (such as AF capabilities planning forums, TSGs, HPTs, Capability Material Teams, ISWGs, etc.). (T-2)

2.9.4.10. Coordinate transition of intelligence requirements, responsibilities and resources as programs transition between research sites, centers or other IC organizations. Draft Intelligence Annex to Transition Support Plans. (T-3)

2.9.4.10. **(AFMC)** Responsible AFMC Center SIOs will coordinate transition of intelligence requirements, responsibilities and resources as programs transition between organizations and supporting intelligence offices. AFMC/A2/5 will assist as necessary on coordination of programs transitioning between Centers. **(T-3).**

2.9.4.11. **(Added-AFMC)** Center SIOs will support the development and implementation of Program Protection Plans (PPPs), Critical Program Information identification, anti-tamper measures, and Supply Chain Risk Management as required by the relevant process owners. AFTC intelligence personnel will collaborate with local test program managers/test security personnel to develop test security plans as required. **(T-3).**

2.9.5. Facilitate Threat Working Groups (TWGs) to identify emerging weapons and technologies that may threaten acquisition programs or the long-term viability (mission effectiveness and survivability) of AF weapon systems in sustainment. Assist, as necessary, with justification for threat-driven modifications to weapon systems, in coordination with program offices and lead command A2 personnel. (T-2)

2.9.5. **(AFMC)** AFMC Center SIOs will host/facilitate program specific or cross-program TWGs to meet program requirements. **(T-2).**

2.9.6. Recommend approval/disapproval to AF/A2 of program requests for waivers to required intelligence planning and threat documentation (e.g. STAR, intelligence mission data or signature support plans, etc.). (T-3)

2.9.6. **(AFMC)** HQ AFMC/A2/5 will recommend approval/disapproval to AF/A2 of program requests for waivers to required intelligence planning and threat documentation (e.g. STAR, intelligence mission data or signature support plans, etc.). **(T-3).**

2.9.6.1. **(Added-AFMC)** HQ AFMC/A2/5 will coordinate on requests for waivers and will prepare AFMC and AF/A2 principals for Air Force Requirements Oversight Councils (AFROCs) and other senior forums. **(T-3).**

2.9.6.2. **(Added-AFMC)** Life-Cycle Mission Data Plan (LMDP) waivers are required for all IMD-dependent programs not preparing LMDPs. **(T-3)**.

2.9.6.3. **(Added-AFMC)** Center SIOs will utilize MFRs to document non-intel sensitive programs. **(T-3).**

2.9.7. Ensure weapon systems in the Operations and Support phase receive threat assessments as needed throughout their lifecycle, to support in-service upgrades relevant to adversaries, reprogramming, and capability advancements. (T-2)

2.9.7.1. **(Added-AFMC)** Acquisition intelligence analysts supporting sustainment activities will identify requirements for threat support using validated threat data or authoritative intelligence from Intelligence Production Centers with production authority for the applicable categories of intelligence. **(T-2).**

2.9.8. Review information provided via AF Form 1067, Modification Proposals, IAW AFI 63-131, Modification Program Management, for systems in sustainment. Determine whether the identified deficiencies/suggested modifications are intelligence sensitive and require intelligence support. (T-2)

2.9.8. **(AFMC)** AFMC Center SIOs will coordinate with operating command intelligence and requirements functions (e.g., ACC/A2 and A8) to help develop, clarify, prioritize and justify requirements associated with weapon systems in sustainment. **(T-2).**

2.9.9. **(Added-AFMC)** AFMC SIOs are the OPRs for acquisition intelligence within their respective centers. **(T-2).**

2.9.9.1. **(Added-AFMC)** AFLCMC, through AFLCMC/IN, will be responsible for acquisition intelligence support across the entire lifecycle process for acquisition programs/systems. **(T-2).**

2.9.9.1.1. **(Added-AFMC)** SIOs supporting weapon systems in the Operations and Support phase will ensure acq intel involvement in legacy/post-Milestone-C programs, to include the following activities unique to sustainment intelligence, as appropriate: **(T-2).**

2.9.9.1.1.1. **(Added-AFMC)** Collaborate with local program office engineers and program managers, and using command intelligence and requirements personnel to assess the vulnerabilities of weapon systems in sustainment in relation to foreign emerging threat weapons and technologies. **(T-2).**

2.9.9.1.1.2. **(Added-AFMC)** Measure baseline configuration of assigned weapon systems against emerging capabilities/technologies. **(T-2).**

2.9.9.1.1.3. **(Added-AFMC)** Provide intelligence support to Weapon System Reviews (WSRs). **(T-2).**

2.9.9.1.1.4. **(Added-AFMC)** Conduct threat assessments on emerging weapons and technologies that may threaten the long-term viability of aircraft/systems in sustainment or components of those systems. These threat assessments will use authoritative intelligence from Intelligence Production Centers (IPCs) with production authority for the applicable categories of intelligence. All threat assessments should be tailored to the needs of the weapon system or its components. **(T-2).**

2.9.9.1.1.5. **(Added-AFMC)** Identify capability gaps in relation to the future battlespace in which legacy aircraft/systems can be expected to operate (during all mission profiles). **(T-2).**

2.9.9.1.1.6. **(Added-AFMC)** Support Life Cycle Management Technology Development Strategy and strategic planning for weapon systems in sustainment. **(T-2).**

2.9.9.1.1.7. **(Added-AFMC)** Provide program offices with research and tailored intelligence analysis regarding submitted and potential POM inputs. **(T-2).**

2.9.9.1.1.8. **(Added-AFMC)** Provide intelligence support to lifecycle management decisions (for example: re-commission, decommission, or modification of self-protection components in response to changes in threat technologies). **(T-2).**

2.9.9.1.1.9. **(Added-AFMC)** Support modeling and simulation activities related to survivability studies for weapon systems in sustainment. **(T-2).**

2.9.9.2. **(Added-AFMC)** AFNWC SIO will be responsible for acquisition intelligence support across the entire lifecycle process for Nuclear Weapons based programs/systems. **(T-2).**

2.9.9.3. **(Added-AFMC)** AFTC unit SIOs will be responsible for acquisition intelligence support to test capabilities and execution processes as follows: **(T-2).**

2.9.9.3.1. **(Added-AFMC)** Provide intelligence information, tools and training support to local test engineers involved in test planning and execution efforts as required; submit RFIs on behalf of test personnel through COLISEUM when necessary to fulfill completion of local intelligence requirements. **(T-2).**

2.9.9.3.1.1. **(Added-AFMC)** To the maximum extent possible, test unit SIOs should identify and prioritize local intelligence sensitive “test programs” to ensure the proper distribution of intelligence support as necessary. This identification and prioritization should be done in collaboration with senior leadership to include the senior engineering staffs where possible. **(T-2).**

2.9.9.3.2. **(Added-AFMC)** Intelligence training and support for local engineering personnel should include foreign threats/technology developments that have a potential for a direct impact on future testing and acquisition programs; goal is to ensure intelligence "situational awareness" is developed throughout the local engineering community as appropriate. **(T-2).**

2.9.9.3.3. **(Added-AFMC)** Provide intelligence information and SME intelligence support to test capability planning, improvement and modernization efforts as required; submit RFIs through COLISEUM to ensure completion of local identified intelligence production support requirements. **(T-2).**

2.9.9.3.4. **(Added-AFMC)** Provide direct SME intelligence support to local engineers tasked with sensor quantification and/or qualification testing as required; assist test planners in obtaining intelligence SME support not locally available as required for successful test planning and execution. **(T-2).**

2.9.9.3.5. **(Added-AFMC)** Directly support test planning and execution by providing necessary expertise and products to support test protection efforts as required; in conjunction with test managers/test security personnel, ensure all necessary elements of testing are properly safeguarded from unauthorized collection. **(T-2).**

2.9.9.3.6. **(Added-AFMC)** Serve as the local liaison between test personnel and the intelligence community support agencies as required; assist local test personnel in making determinations on required intelligence support issues and coordinate direct intelligence requirements and support with intelligence community agencies as required. **(T-2).**

2.9.9.3.7. **(Added-AFMC)** Provide intelligence information, tools and training support to tenant units involved in local acquisition and test processes as required; submit RFIs on behalf of tenant unit personnel through COLISEUM when necessary to fulfill completion of local intelligence requirements. **(T-2).**

2.9.9.3.7.1. **(Added-AFMC)** Tenant unit local intelligence support should be on a non-interference basis with primary test intelligence support mission unless deemed a priority process by the local SIO or Wing Commander. **(T-2).**

2.9.9.3.8. **(Added-AFMC)** Proactively socialize the acquisition intelligence message throughout the test community. Highlight the importance of ensuring intelligence requirements are met in supporting the successful completion of the overall acquisition process; develop collaborative working relationships within the test community and take realistic opportunities to improve overall intelligence supportability efforts. **(T-2).**

2.9.9.4. **(Added-AFMC)** AFRL SIOs will fully integrate acquisition intelligence into the early phase of technology development to ensure intelligence visibility within AFRL developmental planning or S&T research processes, including JUON or other quick reaction projects that do not follow traditional acquisition lifecycle sequences or timelines. AFRL SIOs will identify intelligence dependent technology that is inserted into acquisition efforts and work with PMs to ensure transition and sustainment. **(T-2).**

2.10. **Air Force Operational Test and Evaluation Center (AFOTEC):**

2.10.1. Ensure that Operational Test and Evaluation (OT&E) program threat/target lists and OT&E threat environments are adequately addressed. Ensure appropriate intelligence is used to support test planning and the development of the threat/target/environment (TTE) portions of AFOTEC documents. (T-1)

2.10.2. Participate in STAR TSG, CTA and other acquisition intelligence forums, as appropriate. (T-1)

2.10.3. Coordinate with operating and implementing commands to identify and document total intelligence support requirements for OT&E. Ensure validated threat and ISA are included in Test and Evaluation Master Plans (TEMPs), and Operational Test Plans. (T-1)

2.10.4. Work with MAJCOM/FOA and direct report unit intelligence offices and IC organizations to ensure development of appropriate OT&E threat lists/scenarios to support Initial Operational Test and Evaluation. (T-1)

2.11. **Air Education and Training Command:**

2.11.1. In addition to responsibilities outlined for MAJCOMs/FOAs, design, develop, and instruct acquisition intelligence training courses at the direction of the AF Career Field Manager (CFM). (T-3)

2.11.2. Incorporate acquisition intelligence concepts and materials into acquisition and intelligence training programs at the direction of the appropriate AF CFM. (T-3)

2.12. **Air Force Office of Special Investigations (AFOSI)**

2.12.1. AFOSI will provide input to program protection planners in concert with MAJCOM senior intelligence officers (SIOs) IAW DoDI O-5240.24, *Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA).* (T-0)

2.12.2. Operating or implementing command SIOs will identify counter-intelligence topics, vulnerabilities and opportunities to AFOSI command representative as required. (T-3)

2.12.3. **(Added-AFMC)** AFMC acquisition intelligence analysts will coordinate with AFOSI regarding counter-intelligence input to ISA including protection of critical program information and the supply chain. **(T-3).**

3. IMPLEMENTATION CONCEPTS

3.1. **Acquisition Intelligence Process Requirements.** The following conditions are necessary for intelligence support to be effectively integrated within acquisition life cycle processes:

3.1.1. Common access to and understanding of a program and its intelligence needs, across the intelligence, operations, planning, requirements, research, acquisition and sustainment communities.

3.1.2. Integration of acquisition intelligence stakeholders into assessment, analysis, planning, programming, and decision activities to provide data for cost, schedule and performance tradeoffs.

3.1.3. Tailoring of acquisition intelligence processes to each program. Ensuring they are executed as early as possible in the life cycle, and repeated, as necessary, during the life cycle. As requirements become more defined, more details about intelligence supportability and potential shortfalls can be derived.

3.1.4. The Operations and Support (O&S) phase of a weapon system usually lasts for decades and will encounter evolving theats throughout its life cycle. Warfighters depend on appropriate threat assessments to ensure weapon systems remain mission effective and survivable. Consistent processes during the O&S phase should support needed in-service upgrades relevant to adversaries, including “reprogramming” and capability advancements.

3.2. **Process.** Acquisition intelligence includes the following intelligence considerations for which process checklists and product formats are specified in the AIG:

3.2.1. Intelligence Sensitivity. The first step in the acquisition intelligence process is determination of intelligence sensitivity of the program by the implementing command A2 or delegate. Programs are considered to be intelligence-sensitive if they require intelligence data during development or to perform their mission, require the direct support of intelligence personnel or influence intelligence data at any point in the PCPAD cycle. Criteria and checklists for determining intelligence sensitivity are documented in the AIG. This assessment aids early development of rough-order-of-magnitude estimates for intelligence support to and risk management of the program.

3.2.2. Intelligence Supportability Analysis: ISA is the process by which AF intelligence, acquisition and operations analysts identify, document and plan for requirements, needs and supporting intelligence infrastructure necessary to successfully acquire and employ AF capabilities, thereby ensuring intelligence supportability. It is an iterative, collaborative process that provides tailored support to intelligence sensitive efforts within the Integrated Defense Acquisition, Technology and Logistics Life Cycle Management System. ISA should begin as early as possible and continue throughout the system life cycle; it is to be used for all initiatives, not only ISR programs. It must provide robust support during analysis of alternatives (AoA), system design, production and sustainment and will not end until the final transition/disposal of the capability.

3.2.2.1. ISA results in the identification of derived intelligence requirements (DIRs) and deficiencies, along with associated impacts to both acquisition and operational capability if the required intelligence is not provided. Examples of DIRs include: threat data, geospatial information, PCPAD requirements and issues related to Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF). These analytic activities must be documented, tracked and reported.

3.2.2.1. **(AFMC)** AFMC center SIOs have the responsibility to identify and document DIRs including the projected impact if the intelligence need is not satisfied. DIRs will be recorded for eventual incorporation into an AFMC/A2/5 requirements system of record.

3.2.2.2. Results of ISA form the foundation for intelligence input to requirements and acquisition documents such as Initial Capabilities Documents (ICDs), Capability Development Documents (CDDs), TEMPs, Life Cycle Mission Data Plans (LMDPs), System Requirements Documents, etc., as outlined in applicable acquisition guidance (see Attachment 1).

3.2.2.2. **(AFMC)** AFMC Center SIOs will ensure ISA results are reflected in the proper documents and artifacts.

3.2.2.2.1. **(Added-AFMC)** IMD dependent programs will staff completed LMDPs to their respective Center SIOs.

3.2.2.2.2. **(Added-AFMC)** Center SIOs will route completed LMDPs and waiver requests to the AFMC SIO for review and elevation to approving office.

3.2.2.3. Identified deficiencies are documented and submitted via established IC PRs and AF ISR Capability Planning & Analysis processes for resolution.

3.2.2.3.1. **(Added-AFMC)** AFMC Center SIOs will provide inputs to AFMC/A2/5 regarding ISR capabilities planning and analysis (CPA) inputs.

3.2.3. Documentation. ISA results must be documented throughout the process in a manner that facilitates intelligence input to established requirements systems and required acquisition documents (LCMP, CDD, COLISEUM, etc.) Documentation should be readily available and routinely updated to support acquisition events including, but not limited to: Acquisition Strategy Panels (ASPs), ICDs, CDDs, AF Requirements Boards, and AF Requirements Oversight Council meetings.

3.2.4. Deficiency Resolution. Once intelligence needs, shortfalls, and associated costs/benefits/risks have been assessed, the PM and acquisition intelligence specialists will develop and implement a plan or course of action in a secure and cost-effective manner, in time to meet approved or adjusted MS within the program timeline. The plan or course of action and its supporting information shall be periodically reviewed throughout the life cycle of the program and updated as needed, IAW DoD, Defense Intelligence Agency (DIA), Joint and AF guidance.

3.2.4. **(AFMC)** AFMC Center SIOs will forward unresolved deficiencies to the AFLCMC/IN for CPA and to AFMC/A2/5 for advocacy and resolution.

3.2.5. Intelligence Health Assessment (IHA). The IHA is an assessment of the status of a program's intelligence supportability. IHA factors will be evaluated and incorporated into a program's overall risk assessment.

3.2.5. **(AFMC)** IHAs can be performed at any level to capture ISA results. IHAs may be directed to support programmatic and service level reviews. IHAs should be prepared in timeframes consistent with the program's operations tempo or the occurrence major program events.

3.2.6. Independent Intelligence Assessment (IIA). IIA are objective assessments of capability impact driven by intelligence dependencies that are associated with intelligence-sensitive programs. The IIA is a higher headquarters assessment of impact to acquisition and impact to operations based upon the results of intelligence supportability analysis, CPA and IC responses to acquisition community intelligence requirements.

3.2.6. **(AFMC)** Independent Intelligence Assessment (IIA). The IIA is AFMC/A2/5's overall and independent functional assessment on the acquisition intelligence status of a program. The IIA development is conducted by AFMC/A2/5, which will draw on SMEs from AFMC Center SIOs. IIAs will leverage documented ISA work, but may also take other factors into consideration.

3.2.6.1. **(Added-AFMC)** AFMC/A2/5 will provide copies of IIAs to the appropriate Center SIO(s) of the assessed program(s).

3.2.7. Cross-Program Analysis (CPA). CPA is the examination of programs and derived intelligence requirements to identify commonality and achieve synergies via common solutions. The linkage of documented requirements/shortfalls with multiple customer sets serves to strengthen AF requirements and/or gain efficiencies in meeting these requirements, which can be forwarded to the IC and/or the AF corporate structures for action. CPA can also identify system or program integration issues.

3.2.8. Intelligence Certification. To be accomplished IAW Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3312.01A *Joint Military Intelligence Requirements Certification*.

3.2.8. **(AFMC)** Center SIOs will review JCIDS and ISP documents for completeness, supportability and impact IAW CJCSI 3312.01 criteria. Center SIOs will provide analysis results to the document originator and HQ AFMC/A2/5, and copy AFLCMC/IN for CPA.

3.3. **Primary Collaborative Activities.** The primary means for executing acquisition intelligence are described below. Program teams should tailor the breadth and depth of application of the acquisition intelligence processes to the complexities and needs of their specific effort, commensurate with its point in the life cycle.

3.3.1. Intelligence Support Working Group (ISWG). The ISWG brings together functional representatives from the intelligence, operations and acquisition communities to conduct and document ISA and to assess their collaborative ability to ensure that a program can be adequately supported at a level that will enable mission success. An ISWG is a useful construct to develop intelligence inputs to an AoA.

3.3.1.1. ISWG Participants. The ISWG is established by the program manager and is typically chaired or co-chaired by an implementing command designated intelligence focal point. ISWGs are composed of the following major interest groups: Implementing command program and intelligence offices; lead command requirements and intelligence offices; operational users; system engineers, developers and testers; and intelligence providers (IC representatives, intelligence production center points of contact, intelligence support managers, etc.).

3.3.2. TWGs are working-level integrated product teams (WIPTs) that address threat issues and ensure consistent threat support to acquisition programs throughout their life cycles. They are typically chaired by the program's designated intelligence focal point. TWGs are appropriate forums for addressing TTE issues for all programs. TWGs are typically composed of operational users, intelligence representatives, counterintelligence representatives, systems developers, and system testers.

3.3.3. Cost Analysis Working Group (CAWG). The CAWG is comprised of representatives from operating and implementing command organizations with expertise in cost analysis and works closely with the Air Force Cost Analysis Agency to develop the system life cycle cost estimate. Intelligence cost estimators participate in the CAWG for intelligence sensitive programs.

3.3.3. **(AFMC)** The Intelligence Costing Working Group (ICWG) has developed a tool, the Acquisition Intelligence Lifecycle Cost Estimating Structure (AILCES), to help estimate intelligence costs as early as possible. Chair of the ICWG resides at AFLCMC/IN.

3.3.4. Threat Steering Group (TSG). The TSG's primary purpose is to produce a STAR or STA IAW DoD 5000-series guidance and DIA Instruction (DIAI) 5000.002, *Intelligence Threat Support for Major Defense Acquisition Programs*. **Note:** DIAI 5000.002 is available on SIPRNET at: **http://diateams.dse.dia.smil.mil/sites/Issuances/default.aspx**.

3.3.4.1. TSG membership typically includes representatives from: intelligence staffs of the implementing and operating commands, intelligence staffs of the service and Unified Commands, staff of the program manager; SAF/AQ; DIA (ACAT 1D programs); NASIC; AFOTEC; Operations, Plans and Requirements staffs from the implementing and operating commands, as appropriate.

3.3.4.2. IAW DIAI 5000.002, product centers provide NASIC and the TSG a system description that describe the system in sufficient detail to assess which threats could jeopardize the proposed system's ability to perform its mission. To accurately assess the threat, it is necessary that the system description include mission profiles for all missions foreseen for the system. The program office is responsible for providing the system description. The description must be current.

3.3.5. AoA is an evaluation of the performance, operational effectiveness, operational suitability, and estimated costs of alternative systems to meet a mission capability. The analysis assesses the advantages and disadvantages of alternatives versus the baseline capability, including the sensitivity of each alternative in the available tradespace. Acquisition intelligence has a role in all of the AoA working groups (WG). An ISWG is a useful construct to develop intelligence inputs to an AoA.

3.3.5.1. Threats and Scenarios Working Group (TSWG). The TSWG is responsible for identifying and providing the scenario(s) to be used during an AoA to assess the military utility and operational effectiveness of solutions being considered for possible AF acquisition to meet a valid requirement. Additionally, the TSWG provides threat performance and characteristic information from intelligence sources to enable the AoAs Effectiveness Analysis Working Group (EAWG) to simulate potential threats to mission effectiveness. The TSWG will be staffed primarily with MAJCOM intelligence professionals and SMEs. Members support the TSWG by providing relevant intelligence information to sustain TSWG decisions. The TSWG is the forum tasked to track, anticipate, and mitigate issues potentially impacting the identification, selection and recommendation of scenarios to the AoA WIPT. Other members may be added on an ad hoc basis to resolve issues, as they arise.

3.3.5.2. Technology and Alternatives Working Group (TAWG). The TAWG acts as the interface with alternative providers, crafting the requirements request, receiving alternative data, and resolving questions between the providers and the rest of the AoA WGs. The acquisition intelligence specialist's role as a TAWG member is to ensure the requirements information request specifically asks for ISR capability enabler assumptions to include external infrastructure needs, these include inputs from the acquisition intelligence costs analyst detailing what data is required to frame the ISR infrastructure costing analysis report.

3.3.5.3. Operating Concept WG. The acquisition intelligence specialist’s role is to review the CONOPS from an intelligence perspective to ensure intelligence supportability issues/needs are noted.

3.3.5.4. Effectiveness Analysis Working Group. The acquisition intelligence specialist participates in the creation of the analysis assumptions from the perspective of valid intelligence supportability.

3.3.5.5. Cost Analysis Working Group. Acquisition intelligence cost analysts, in coordination with, members of the other working groups, support the AoA by providing cost data on intelligence support-related activities external to the proposed solutions/alternatives (i.e. DOTMLPF).

3.3.6. Other Supported Venues. Other acquisition-related forums that can require intelligence support include Acquisition Strategy Panels, Systems Security Working Groups, HPTs, Integrated Test Teams, Interoperability WGs, and unique WGs established by programs/capabilities/initiatives/projects.

LARRY D. JAMES, Lt Gen, USAF
Deputy Chief of Staff, Intelligence, Surveillance,
and Reconnaissance

(AFMC)

RANDY E. BROWN, SES, DAF
Director of ISR and Requirements

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 10-9, *Lead Command Designation and Responsibilities for Weapons Systems*, 8 March 2007

AFPD 14-1, *Intelligence, Surveillance, and Reconnaissance (ISR) Planning, Resources, and Operations*, 2 April 2004

AFPD 16-7, *Special Access Program*, 19 February 2014

AFPD 63-1, *Acquisition and Sustainment Life Cycle Management*, 3 April 2009

AFPD 90-11, *Strategic Planning System*, 26 March 2009

AFPD 99-1, *Test and Evaluation Process*, 22 July 1993

AFI 10-601, *Operational Capability Requirements Development*, 6 November 2013

AFI 14-201, *Intelligence Production and Applications*, 1 December 2002

AFI 14-205, *Geospatial Information and Services*, 5 May 2010

AFI 16-701, *Military Personnel Exchange Program (MPEP)*, 2 February 2006

AFI 33-360, *Publications and Forms Management*, 25 September 2013

AFI 36-2640, *Executing Total Force Development*, 16 December 2008

AFI 63-101, *Acquisition and Sustainment Life Cycle Management*, 20 June 2013

AFI 63-114, Quick Reaction Capability Process, 4 January 2011

AFI 63-131, *Modification Program Management*, 19 March 2013

AFI 63-1201, *Life Cycle Systems Engineering*, 23 July 2007

AFI 99-103, *Capabilities-Based Test and Evaluation*, 16 October 2013

AFI 99-114, *Foreign Materiel Program*, 25 October 2002

AFMAN 33-363, *Management of Records*, 1 March 2008

DoDI 5000.02, *Operation of the Defense Acquisition System*, November 25, 2013

DoDI 5200.39, *Critical Program Information (CPI) Protection Within the Department of Defense*, July 16, 2008

DoDI O-5240.24, *Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)*, June 8, 2011

DoDD 5250.01, *Management of Intelligence Mission Data (IMD) Within the DoD*, January 22, 2013

CJCSI 3170.01G, *Joint Capabilities Integration and Development System; Chairman of the Joint Chiefs of Staff Manual for the Operation of the Joint Capabilities Integration and Development System*, March 1, 2009

CJCSI 3312.01A, *Joint Military Intelligence Requirements Certification*, February 23, 2007

DIAI 5000.002, *Intelligence Threat Support for Major Defense Acquisition Programs* January 19, 2005

AIG, *Acquisition Intelligence Guidebook*

Adopted Forms

AF Form 847, *Recommendation for Change of Publication,* 22 September 2009

AF Form 1067, *Modification Proposals,* 1 November 1999

Abbreviations and Acronyms

ACAT—Acquisition Category

AF—United States Air Force

AFI—Air Force Instruction

AFISRA—Air Force Intelligence, Surveillance and Reconnaissance Agency

AFMC—Air Force Materiel Command

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigations

AFOTEC—Air Force Operational Test and Evaluation Center

AFPD—Air Force Policy Directive

AFSPC—Air Force Space Command

AIG—Acquisition Intelligence Guidebook

AoA—Analysis of Alternatives

ASP—Acquisition Strategy Panel

AT&L—Acquisition, Technology and Logistics

CAWG—Cost Analysis Working Group

CDD—Capability Development Document

CFM—Career Field Manager

CI—Counterintelligence

CIA—Central Intelligence Agency

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

CONOPS—Concept of Operations

CPA—Cross-Program Analysis

CPD—Capability Production Document

CTA—Capstone Threat Assessment

DAO—Designated Acquisition Official

DIA—Defense Intelligence Agency

DIAI—Defense Intelligence Agency Instruction

DIAP—Defense Intelligence Analysis Program

DIR—Derived Intelligence Requirements

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DOTMLPF—Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities

DS&TI—Designated Science and Technology Information

EAWG—Effectiveness Analysis Working Group

FBI—Federal Bureau of Investigations

FOA—Field Operating Agency

GEOINT—Geospatial Intelligence

HPT—High Performance Team

IAW—In Accordance With

IC—Intelligence Community

ICD—Initial Capabilities Document

IIA—Independent Intelligence Assessment

IHA—Intelligence Health Assessment

IMD—Intelligence Mission Data

IOC—Initial Operational Capability

ISA—Intelligence Supportability Analysis

ISR—Intelligence, Surveillance, and Reconnaissance

ISWG—Intelligence Support Working Group

JCIDS—Joint Capabilities Integration and Development System

KSA—Key System Attribute

LMDP—Life Cycle Mission Data Plan

MAJCOM—Major Command

MCIA—Marine Corps Intelligence Activity

MDAP—Major Defense Acquisition Program

MS—Milestone

MSIC—Missile and Space Intelligence Center

M&S—Modeling & Simulation

NASIC—National Air and Space Intelligence Center

NGA—National Geospatial-Intelligence Agency

NGIC—National Ground Intelligence Center

NRO—National Reconnaissance Office

NSA—National Security Agency

OPR—Office of Primary Responsibility

OT&E—Operational Test and Evaluation

O&M—Operation and Maintenance

O&S—Operations and Sustainment

PCPAD—Planning and direction, Collection, Processing and exploitation, Analysis and production, and Dissemination

PEO—Program Executive Officer

PM—Program Manager

PMD—Program Management Directive

PPBE—Planning, Programming, Budgeting, and Execution System

PPP—Program Protection Plan

PR—Production Requirement

SAF/AQ—Assistant Secretary of the Air Force for Acquisition

SIO—Senior Intelligence Officer

SME—Subject Matter Expert

STA—System Threat Assessment

STAR—System Threat Assessment Report

T-0—Tier 0

T-1—Tier 1

T-2—Tier 2

T-3—Tier 3

TAWG—Technology and Alternatives Working Group

TEMP—Test and Evaluation Master Plan

TPP—Technology Protection Plan or Planning

TSG—Threat Steering Group

TSWG—Threats and Scenarios Working Group

TTE—Threat, Target, Environment

TWG—Threat Working Group

USAF—United States Air Force

USD (AT&L)—Under Secretary of Defense for Acquisition, Technology and Logistics

WG—Working Group

WIPT—Working Level Integrated Product Team

Terms

Acquisition Intelligence Specialist—Personnel certified in acquisition intelligence.

Analysis of Alternatives (AoA)—The evaluation of the operational effectiveness and estimated costs of alternative materiel systems to meet a mission need. The analysis assesses the advantages and disadvantages of alternatives being considered to satisfy requirements, to include the sensitivity of each alternative to possible changes in key assumptions or variables. The AoA assists decision-makers in selecting the most cost-effective materiel alternative to satisfy a mission need.

Authoritative—An intelligence product that has been published/posted under the auspices of the Defense Intelligence Analysis Program (DIAP). It has been produced by the intelligence element recognized in the DIAP as the authority for that kind of information, vetted and adjudicated within that element, and is based on reliable and trusted analysis tools and processes.

Capability—The combined capacity of personnel, materiel, equipment, and information in measured quantities, under specified conditions, that, acting together in a prescribed set of activities, can be used to achieve a desired output.

Capability Development Document (CDD)—A document that captures the information necessary to develop a proposed program, normally using an evolutionary acquisition strategy. The CDD outlines an affordable increment of militarily useful, logistically supportable and technically mature capability. The CDD is validated and approved before MS B.

Capability Production Document (CPD)—A document that addresses the production elements specific to a single increment of an acquisition program. The CPD is validated and approved before MS C.

Capstone Threat Assessment (CTA)—The DoD Intelligence Community's official assessment of the principal threat systems and capabilities within a category of warfare (e.g., air, Space, Cyber, Naval Warfare, etc.) that a potential adversary might reasonably bring to bear in an attempt to defeat or degrade U.S. weapon systems. CTAs project the threat environment in a given warfare area out to 20 years, and constitute the validated, DoD IC position with respect to those warfare areas.

Critical Intelligence Parameter (CIP)—A factor which clearly defines the threshold at which the performance of a foreign system/capability could compromise the program / mission effectiveness of the US system. If a CIP is breached (i.e., a foreign system has met the CIP threshold) materiel and/or non-materiel (DOTMLPF) changes must be considered, the program will likely require additional time and funds to adjust (“re-baseline”), and spiral/increment thresholds, objectives, KPPs, KSAs, etc. may require adjustment.

Cross-Program Analysis (CPA)—CPA is an analytical effort designed to "look across" all intelligence-sensitive programs and the related intelligence shortfalls. The primary objective of CPA is to identify and consolidate like deficiencies. Synergies between programs and cost savings are realized when solutions are identified that support multiple programs. The results of CPA guide identification and development of solutions to the documented deficiencies. An additional aspect of CPA is to identify system or program integration issues.

Defense Intelligence Analysis Program (DIAP)—DIA centrally manages defense intelligence analysis and production using a distributed analytical process known as the DIAP. This program integrates general military intelligence and scientific and technical intelligence production conducted at DIA, Combatant Commands, and Service intelligence centers. The DIAP allows DIA to focus all-source defense intelligence analysis efforts on compelling issues for defense customers while limiting duplication of effort.

Derived Intelligence Requirements——Intelligence requirements that are implied from higher-level requirements, such as Key Performance Parameters (KPPs) and Key Systems Attribute (KSA).

Geospatial Intelligence—The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information, also called GEOINT.

Implementing Command—The command or agency designated by the AF Acquisition Executive to manage an acquisition program. The intelligence support to the manager of an acquisition program usually resides with the Product Center/Logistics Center/Lab Research Site Intelligence Division/Branch.

Initial Capabilities Document (ICD)—Documents the need for a materiel approach to a specific capability gap derived from an initial analysis of materiel approaches executed by the operational user and, as required, an independent analysis of materiel alternatives. It guides initial program activities and supports MS A.

Intelligence Community (IC)—The federation of executive branch agencies and organizations that conduct foreign and/or counter-intelligence activities necessary for conduct of foreign relations and protection of national security. IC members include the Service intelligence organizations (NGIC, ONI, NASIC, MCIA, and Service intelligence staff/support units), NSA, CIA, FBI, DIA (including MSIC and AFMIC), NRO, and NGA, as well as the intelligence components of the US Coast Guard, Department of Energy, Department of Homeland Security, Department of State, Department of Commerce, and Department of Treasury. **Note:** Counterintelligence (CI) is an organizational and functional part of the Intelligence Community, but is usually "compartmented" from foreign intelligence offices and/or functions in order to protect sensitive personal and law enforcement information IAW federal law and Intelligence Oversight guidance. While this AFI focuses on support from the (foreign) intelligence components of the IC, representatives from the CI components can be requested to support acquisition intelligence processes, if needed. The Air Force Office of Special Investigations (AFOSI) is the primary USAF CI organization, a FOA that identifies, investigates and neutralizes criminal, terrorist, and espionage threats to the personnel and resources of USAF and DoD.

Intelligence Costing——An integral part of the ISA is the estimation of costs associated with the Intelligence resources required to support the acquisition programs. The lack of understanding of these costs can result in scheduling delays, costly work-arounds, and unplanned adjustments to Operations and Maintenance (O&M) budgets.

Intelligence Estimate—An appraisal of available intelligence relating to a specific situation or condition, with a view to determining the courses of action open to an enemy or potential enemy and the probable order of adoption of such courses of action.

Intelligence Mission Data (IMD)—DoD intelligence used for programming platform mission systems in development, testing, operations, and sustainment including, but not limited to, the following functional areas: signatures, EWIR, OB, C&P, and GEOINT.

Intelligence Requirement—The need for a product, function, infrastructure, or service provided by the Intelligence Community (IC) that is integral to a program at a point within its life cycle. Intelligence requirements can come from any part of the DOTMLPF construct. Program intelligence requirements should be documented to support both current and future acquisition and intelligence requirements. Documentation should include information on the availability of the needed IC capabilities. Requirements which cannot be met with current IC capabilities are identified as gaps, shortfalls or deficiencies.

Intelligence-sensitive—Any program/initiative that produces, consumes, processes, or influences intelligence information, thereby requiring threat or intelligence infrastructure support. If it is likely that, in the future, the program would produce, consume, process, or influence intelligence information, it should be considered intelligence-sensitive.

Intelligence Supportability—Refers to the availability, suitability and sufficiency of intelligence support required by a program. CJCSI 3312 Par. 4.c(2)(b).

Intelligence Supportability Analysis (ISA)——Intelligence personnel partner with acquisition and operations stakeholders, and with other SMEs, to help derive/resolve the intelligence requirements by tailoring and utilizing the acquisition intelligence processes described in this AFI. In addition, IAW CJCSI 3312.01, the AF must review the intelligence support and intelligence-related operational requirements specified in (or derived from) JCIDS and other acquisition documents for completeness, supportability, and impact. For the purposes of this AFI, these intelligence certification activities are also included under the "ISA" term. ISA was formerly known as intelligence infrastructure analysis.

Intelligence Support Working Group (ISWG)—The ISWG is an enduring and continuously functioning group that brings together functional representatives from the intelligence, operations and acquisition communities to conduct and document ISA and to assess their collaborative ability to ensure that a program can be adequately supported at a level that will enable mission success.

Intelligence, Surveillance, and Reconnaissance (ISR)—Term referring to the activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function.

JCIDS Documents (ICD, CDD, CPD)——IAW CJCSI 3170.01 and the JCIDS Manual, DIA validates the threat and intelligence supportability information in all JROC Interest, JCB Interest, and Joint Integration ICDs, CDDs and CPDs through the intelligence certification process (ref. CJCSI 3312.01). For programs with Joint Information or Independent JPDs, which DIA does not review or validate, DoD Components can utilize DIA-validated threat reference information and/or data contained in DoD Service validated and authoritative intelligence products for their JCIDS documents.

Life Cycle—The span of time associated with a technology, concept, system, subsystem, capability, initiative or end-item that begins with the conception and initial development of the requirement, continues through development, acquisition, fielding, sustainment, until the time it is either consumed in use or disposed of as being excess to all known materiel requirements.

Life Cycle Mission Data Plan (LMDP)—A management plan that is applied throughout the life of a intelligence mission data-dependent acquisition that bases programmatic decisions on the availability of data over the life of a mission data-dependent acquisition.

Major Defense Acquisition Program (MDAP)—A DoD acquisition program that is not a highly sensitive classified program and: (1) That is designated by the USD(AT&L) as a MDAP; or (2) That is estimated to require an eventual total expenditure for research, development, test, and evaluation, including all planned increments, of more than $365 million (based on fiscal year 2000 constant dollars) or an eventual total expenditure for procurement, including all planned increments, of more than $2.19 billion (based on fiscal year 2000 constant dollars).

Milestone (MS)—Major decision point that separates the phases of an acquisition program under the DoDI 5000.02, *Operation of the Defense Acquisition System,* acquisition management framework. These include: MS A—Technology Development Phase approval; MS B—Engineering and Manufacturing Development Phase approval (normally the initiation of an acquisition program); and MS C—Production and Deployment Phase approval.

Planning, Programming, Budgeting, and Execution System (PPBE)—A cyclic process containing four distinct but interrelated phases: Planning—Produces a fiscal forecast, planning guidance, and program guidance; Programming—Creates the AF portion of the DoD's Future Years Defense Program (FYDP) by defining and examining alternative forces and weapons and support systems; Budgeting—Formulates and controls resource requirements, allocation, and use; and Execution—Measures and validates the performance of the planning, programming, and budgeting phases.

Program—For clarity throughout this publication, a program, project, technology demonstration, research effort, development planning activity, quick reaction capability, study, concept, initiative, system, modification, sustainment effort or upgrade involving intelligence support during research, development, acquisition, test, modernization, or sustainment will be implied by and referred to by the word “program.”

Program Management Directive (PMD)—The official AF document used to direct acquisition responsibilities to the appropriate major commands, agencies, program executive office, or designated acquisition commander. All acquisition programs require PMDs. PMDs initiate and terminate actions, cite funding sources, and assign responsibilities and tasks to appropriate commands and agencies.

Program Protection Plan or Planning (PPP)—The Program Protection Plan is the program manager's single source document used to coordinate and integrate all protection efforts designed to protect critical information and resources, and to prevent inadvertent disclosure of leading edge technology to foreign interests. Program Protection Planning is a comprehensive effort that encompasses all security, technology transfer, intelligence, and counterintelligence processes through the integration of embedded system security processes, security manpower, equipment, and facilities.

Requirements Strategy—A plan or document that maps the details necessary for developing a requirements document, and describes the resources and communities necessary to support the process.

Special Access Program (SAP)—A program established by the head of a department or agency whom the President has designated in the Federal Register as an original SECRET or TOP SECRET classification authority, which has additional "need to know" access controls beyond those controls normally required for access to information classified as CONFIDENTIAL, SECRET or TOP SECRET. SAPs are established only when the program is required by statute or upon a specific finding that: (1) the vulnerability of, or threat to, specific information is exceptional; and (2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure.

System Threat Assessment Report (STAR)—Official assessment of the principal threat systems and capabilities that a potential adversary might reasonably be expected to employ in an attempt to defeat or degrade a specific US weapon system when it is deployed. The STAR includes descriptions of the operational threat environment, target attributes, system-specific threats (for the time period of IOC to IOC+10 years), and emergent technologies. STARs are developed for ACAT Level 1D, 1C, and ACAT II programs, and for all programs on DOT&E Oversight List. For those AF programs, STARs are required for Milestones (MS) B and C IAW DoDI 5000.02. AF policy: STARs must be current at the time each MS decision is made. STARs typically expire 24 months from the date of publication.

Technology Protection Plan or Planning (TPP)—Similar to the PPP developed in the acquisition cycle, a TPP is developed by research organizations to identify critical information and resources that require increased protection. The TPP identifies the threats to a technology and prescribes necessary countermeasures to ensure the technology is adequately protected from compromise. TPPs will likely focus on those critical technologies, information, capabilities, and demonstrations, referred to as designated science and technology information (DS&TI), that have a more defined transition path to an activity ready to assume program management responsibility (usually an acquisition program or other DoD government agency or organization) or that have strong potential for transition based on the underlying value/advancement of warfighter capability. DS&TI will be protected via a TPP or, in the case of a technology insertion Advanced Technology Demonstration, within the auspices of an existing Program Protection Plan (PPP). The overall objective of AFRL-generated technology protection planning is to protect identified DS&TI that will transition into a weapons system platform or program to ensure the AF can acquire, field, and operate quality weapons and support systems, which have not been compromised and will meet mission requirements.

Tier 0 (T-0)—Determined by respective non-AF authority (e.g., Congress, White House, OSD, JS). The requirement is external to AF. Requests for waivers must be processed through command channels to publication OPR for consideration. (AFI 33-360)

Tier 1 (T-1)—Non-compliance puts Airmen, commanders or the AF strongly at risk of mission or program failure, death, injury, legal jeopardy or unacceptable fraud, waste or abuse. T-1 waiver requests may be granted at the MAJCOM/CC level, but may not be delegated lower than MAJCOM Director, with the concurrence of the publication's approving official. (AFI 33-360)

Tier 2 (T-2)—Non-compliance has the potential to create moderate risk of mission or program degradation or failure, injury, legal jeopardy or unacceptable fraud, waste or abuse. Waivers may be granted at the MAJCOM/CC level, but may not be delegated lower than MAJCOM Director. (AFI 33-360)

Tier 3 (T-3)—Non-compliance has a relatively remote potential to create risk of mission or program degradation or failure, injury, legal jeopardy or unacceptable fraud, waste or abuse. Waivers may be granted at the Wing/DRU/FOA/CC level. (AFI 33-360)

Attachment 1 (AFMC)

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 14-111, *Intelligence Support to the Acquisition Life-Cycle*, 18 May 2012

CJCSI 3312.01B, *Joint Military Intelligence Certification*, February 23, 2007

Prescribed Forms

There are no Prescribed Forms for this publication

Adopted Forms

There are no Prescribed Forms for this publication

Abbreviations and Acronyms

ACC —Air Combat Command

AETC —Air Education and Training Command

AFLCMC —Air Force Life-Cycle Management Center

AFNWC —Air Force Nuclear Weapons Center

AFRC —Air Force Reserve Corps

AFRIMS —Air Force Records Information Management System

AFRL —Air Force Research Lab

AFROC —Air Force Requirements Oversight Council

AFSC —Air Force Sustainment Center

AFTC —Air Force Test Center

AILCES —Acquisition Intelligence Life-cycle Cost Estimating Structure

COLISEUM —Community On-Line Intelligence System for End Users and Managers

CPI —Critical Program Information

DP —Development Planning

FMS —Foreign Military Sales

ICWG —Intelligence Costing Working Group

IMA —Individual Mobilization Augmentee

IPC —Intelligence Production Center

IQT —Initial Qualification Training

ISP —Information Support Plan

JUON —Joint Urgent Operational Need

MFR —Memorandum for Record

MQT —Mission Qualification Training

POM—Program Objective Memorandum

QRC —Quick Reaction Capability

RDS —Records Disposition Schedule

RFI —Request for Information

SAP -Special Access Program

S&T —Science and Technology

WSR —Weapon System Review

Terms

Community On-line Intelligence System for End Users and Managers (COLISEUM)—A DIA automated production/requirements management system designed to support the Intelligence Community for registration, validation, tracking and management of DOD/Joint/Service Production Requirements (PRs), otherwise known as Requests for Information (RFIs). Access is available through the TS//SCI-level Joint Worldwide Intelligence Communication System (JWICS) network.

High Performance Team (HPT)—A HPT convenes to capture, articulate, and document the operator's requirements in minimum time, while achieving stakeholder buy-in. Ideally, the HPT will consist of 7-11 core participants, which includes a lead (the sponsor, during a requirements development HPT), a facilitator, Air Force Subject Matter Experts (SMEs) (i.e., operators, systems engineers, acquirers, testers, logisticians, intelligence support managers, etc.), government agencies and other Services (as required), and support team members (not physically present but available via phone or e-mail for reach back).

Independent Intelligence Assessment:—IIA is an independent IHA at the MAJCOM level.

Intelligence Certification—The affirmation that requirements for intelligence support have been completely and adequately declared and identified; adequately assessed for projected supportability; that critical intelligence supportability or threat-related issues identified during coordination of program documents have been addressed; and that any projected shortcomings in intelligence support will be dealt with in an appropriate manner. This certification occurs as a prerequisite for the Joint Capabilities Integration and Development System and defense acquisition processes, and occurs at each acquisition milestone.

Intelligence Costing——An integral part of the ISA is the estimation of costs associated with the Intelligence resources required to support the acquisition programs. The lack of understanding of these costs can result in scheduling delays, costly work-arounds, and unplanned adjustments to Operations and Maintenance (O&M) budgets.

Intelligence Health Assessment—IHAs use a checklist to scrutinize programs/projects/ initiatives, systems, and capabilities deemed to be intelligence-sensitive (i.e., that are either users or producers of intelligence) to identify any potential risks, which left uncorrected might result in program delays, cost over-runs or degraded system capability. During the ISA process, the analyst should be working with and providing risk assessments to the program office. The IHA can be provided to the program manager in the form of a briefing or MFR. The IHA should be incorporated into the program's overall risk assessment and address cost, schedule, and performance.

Intelligence-sensitive—Any program/initiative that produces, consumes, processes, or influences intelligence information, thereby requiring threat or intelligence infrastructure support. If it is likely that, in the future, the program would produce, consume, process, or influence intelligence information, it should be considered intelligence-sensitive.

Intelligence, Surveillance, and Reconnaissance (ISR)—Term referring to the activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function.

Threat Working Group—TWGs are working-level IPTs, with similar membership as that of TSGs, that are held as required to discuss threat issues and ensure consistent threat support to acquisition programs throughout their life cycle.